



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/642,879	08/21/2000	Stephen Michael Matyas JR.	5577-208	8114

20792 7590 04/22/2004

MYERS BIGEL SIBLEY & SAJOVEC  
PO BOX 37428  
RALEIGH, NC 27627

EXAMINER

TRAN, ELLEN C

ART UNIT	PAPER NUMBER
----------	--------------

2134

DATE MAILED: 04/22/2004

2

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

09/642,879

Applicant(s)

MATYAS ET AL.

Examiner

Ellen C Tran

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 21 August 2000.  
2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.  
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-66 is/are pending in the application.  
4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.  
5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.  
6) ☒ Claim(s) 1-66 is/are rejected.  
7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.  
8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

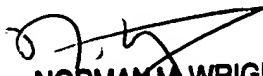
**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.  
10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).  
11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
a) ☐ All b) ☐ Some \* c) ☐ None of:  
1. ☐ Certified copies of the priority documents have been received.  
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

  
NORMAN M. WRIGHT  
PRIMARY EXAMINER

**Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892)  
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)  
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_.  
4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_.  
5) ☐ Notice of Informal Patent Application (PTO-152)  
6) ☐ Other: \_\_\_\_\_.

**DETAILED ACTION**

1. This action is responsive to communication: original application filed  
21 August 2000.

2. Claims 1-66 are currently pending in this application. Claims 1, 17, 29, 41, 53, 65 and 66  
are independent claims.

***Claim Rejections - 35 USC § 102***

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the  
basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on  
sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 1, 3-5, 9-20, 24-29, 31-44, 48-53, 55-66 are rejected under 35 U.S.C. 102(b) as  
being anticipated by Narasimhalu et al. U.S. Patent No. 5,499,298 (hereinafter '298).

As to independent claim 17, “A method for controlling access to digital data of a file  
utilizing a file system including a personal key client, wherein the personal key client  
carries out the steps of: generating an encryption key; encrypting the digital data of the file  
with the encryption key” is taught in '298 col. 5, lines 35-47;

“obtaining a password associated with the file; generating a personal key from the  
password associated with the file; encrypting the encryption key with the personal key;  
incorporating in a file header the encryption key encrypted with the personal key” is shown  
in '298 col. 11, lines 1-5 (i.e. “password” same as “valid CID”);;

“requesting encryption of the file header with a control key; receiving the file  
header encrypted with the control key; associating the file header with the file; and storing

**the file header and the encrypted digital data of the file at a file server”** is disclosed in ‘298 col. 6, lines 21-45.

As to dependent claim 18, **“further comprising: receiving access requests from a user to access the file system; determining if the access request is authorized”** is taught in ‘298 col. 11, lines 13-15;

**“providing a ticket utilized to access the file system if the access request is authorized”** is shown in ‘298 col. 9, lines 7-10

**“and utilizing the ticket to perform file storage, access and administrative operations”** is disclosed in col. 11, lines 33-60.

As to dependent claim 19, **“further comprising the steps of: receiving a request to access the file by the file owner; requesting the file and the associated file header from the file server”** is disclosed in ‘298 col. 11, lines 1-2;

**“extracting the encryption key encrypted with the personal key and the control key from the file header; requesting recovery of the encrypted encryption key from the file header; receiving the recovered encrypted encryption key”** is taught in ‘298 col. 7, lines 60-67;

**“obtaining a password to decrypt the file; generating the personal key from the obtained password; decrypting the recovered encrypted encryption key with the personal key to recover the encryption key; and decrypting the encrypted digital data with the recovered encryption key”** is taught in ‘298 col. 11, lines 1-5 (i.e. “password” same as “valid CID”).

**As to dependent claim 20, “further comprising the steps of: requesting the file header associated with the file from the file server; receiving the file header from the file server; extracting the encryption key encrypted with the personal key and the control key; requesting recovery of the encrypted encryption key; receiving the recovered encrypted Encryption key; generating the personal key; decrypting the recovered encrypted encryption key with the personal key to provide a recovered encryption key; obtaining a new password associated with the file; generating a new personal key based on the new password; encrypting the recovered encryption key to provide a new personal key encrypted encryption key; requesting an update of the file header to incorporate the new personal key encrypted encryption key; receiving an updated file header from the personal key server; and providing the updated file header to the file server” is taught in ‘298 col. 11, lines 31-60 (i.e. “new password” same as “re-encrypts using the COIN using key  $K_{T+1}$ ”)**

**As to dependent claim 24, “wherein the step of requesting encryption of the file header with a control key is preceded by the step of incorporating the encryption key unencrypted in the file header; and the method further comprising: providing a list of users authorized to have access to the file” is shown in ‘298 col. 2, lines 60-67.**

**As to dependent claim 25, “further comprising: receiving a request to access the file by a user other than the file owner; requesting the file and” is disclosed in ‘298 col. 10, lines 11-28;**

**“the associated file header from the file server” is taught in ‘298 col. 5, lines 4-15;**

**“extracting the encryption key encrypted with only a control key from the file header; requesting recovery of: the encryption key from the file header; receiving the**

**recovered encryption key; and decrypting the encrypted digital data with the recovered encryption key” is shown in ‘298 col. 7, lines 60-67.**

**As to dependent claim 26, “wherein the step of requesting encryption of the file header with a control key is preceded by the steps of: encrypting the encryption key with a public key of each user other than the owner which is authorized to access the file to provide a public key encrypted encryption key corresponding to each user other than the owner; incorporating the public key encrypted encryption key corresponding to each user other than the owner of the file in the file header; and the method further comprising: providing a list containing each user authorized to have access to the file” is disclosed in ‘298 col. 6, lines 1-12.**

**As to dependent claim 27, “further comprising: requesting the file header associated with the file from the file server; receiving the file header from the file server; extracting the encryption key encrypted with the personal key and the control key from the received file header; requesting recovery of the encrypted encryption key; receiving the recovered encrypted encryption key; generating the personal key; decrypting the recovered encrypted encryption key with the personal key to provide a recovered encryption key; obtaining a new public: key associated with a user other than the owner of the file; encrypting the recovered encryption key with the new public key to provide a new public: key encrypted encryption key; requesting an update of the file header to incorporate the new public key encrypted encryption key; receiving an updated file header; and providing the updated file header to the file server” is taught in ‘298 col. 11, lines 31-60.**

**As to dependent claim 28, “receiving a request from a user other than the owner to access the file; requesting the file and the associated file header from the file server; receiving the encrypted file and the file header from the file server; extracting the public key encrypted encryption key encrypted with the control key corresponding to the user requesting access to the file from the file header; requesting recovery of the public key encrypted encryption key corresponding to the user requesting access to the file from the file header; receiving the recovered public key encrypted encryption key; obtaining a private key associated with the user requesting access to the file; decrypting the recovered encrypted encryption key with the private key to recover the encryption key; and decrypting the encrypted digital data with the recovered encryption key” is shown in ‘298 col. 11, lines 1-11.**

**As to dependent claim 29, “A method for controlling access to digital data of a file in a file system having a personal key server” is taught in ‘298 col. 5, lines 4-15;**

**“the personal key server carrying out the steps of receiving a request from a requester to create a file header associated with the file, the request containing an encryption key encrypted with a personal key” is shown in ‘298 col. 6, lines 1-15;**

**“encrypting the encrypted encryption key with a control key to provide the file header containing an encryption key encrypted with both a personal key and a control key; and returning the file header to the requestor” is disclosed in ‘298 col. 5, lines 35-47.**

**As to dependent claims 31, 35, and 39, these claims contain substantially subject matter as above claim 17 and are rejected along the same rational.**

As to dependent claim 32, “further comprising: receiving a request to update the file header to incorporate an encryption key encrypted with a new encryption key; encrypting the encryption key encrypted with the new encryption key with the control key to provide a control key encrypted new encryption key encrypted encryption key; incorporating the control key encrypted new encryption key encrypted encryption key in the file header to provide an updated file header; and returning the updated file header” is taught in ‘298 col. 10, lines 32-46.

As to dependent claim 33, “wherein the request to update of the file header to incorporate the encryption key encrypted with a new encryption key includes an identification of a user requesting to update the file header, the method further comprising: comparing the identification of the user requesting to update the file header with a list of users authorized to access the file; and rejecting the request if the user requesting to update the file header is not identified in the list of users authorized to access the file as the owner of the file” is shown in ‘298 col. 10, lines 32-46 (i.e. “identification of a user” same as “CID”).

As to dependent claim 34, “wherein the request from a requestor to create a file header associated with the file, further contains an unencrypted encryption key associated with users authorized to access the file, the method further comprising: encrypting the unencrypted encryption key with the control key; incorporating the unencrypted encryption key encrypted with the control key in the file header; and returning the file header incorporating the encryption key encrypted with the control key” is disclosed in ‘298 col. 6, lines 41-43 (i.e. “unencrypted encryption key” same as “public key DPK”)



As to dependent claim 36, “wherein the request to recover the encryption key includes an identification of the user requesting to access the file, the method further comprising: comparing the identification of the user requesting to access the file with a list of users authorized to access the file; and rejecting the request if the user requesting to access the file is not identified in the list of users authorized to access the file” is taught in ‘298 col. 11, lines 1-30.

As to dependent claim 37, “wherein the request to create a file header associated with the file includes a public key encrypted encryption key corresponding to each user authorized to access the file other than an owner of the file and a list containing each user authorized to have access to the file, the method further comprising: encrypting each public key encrypted encryption key with the control key; incorporating each public key encrypted encryption key encrypted with the control key in the file header; returning the file header incorporating each public key encrypted encryption key encrypted with the control key” is shown in ‘298 col. 11, lines 1-11.

As to dependent claim 38, “further comprising the step of creating an access control list from the list provided with the request” is disclosed in ‘298 col. 11 lines 13-30 (i.e. “access control list” same as “one of the AWs found in field 142”).

As to dependent claim 40, “further comprising: comparing the identification of the user requesting to access the file with the list of users authorized to access the file; and rejecting the request if the user requesting to access the file is not identified in the list of users authorized to access the file” is taught in ‘298 col. 11, lines 1-30.

**As to independent claim 1**, this claim is directed to the system of methods 17 and 29 and is rejected along similar rationale.

**As to dependent claims 3-5 and 9-16**, these claims incorporate substantially similar as claims 17-20, 24-29, and 31-40 above and are rejected along the same rationale.

**As to independent claim 41**, this claim is directed to a personal key client for the system of method of 17 and is rejected along the same rationale.

**As to dependent claims 42-44 and 48-52**, these claims incorporate substantially similar subject matter as above claims 18-20 and 24-28 above and are rejected along the same rationale.

**As to independent claim 53**, this claim is directed to a personal key server system of the method of claim 29 and is rejected along the same rationale.

**As to dependent claims 55-64**, these claims incorporate substantially similar subject matter as claims 31-40 and are rejected along the same rationale.

**As to independent claim 65**, this claim is directed to a computer program product of the method of claim 17 and is rejected along the same rationale.

**As to independent claim 66**, this claim is directed to a computer program product of the method of claim 29 and is rejected along the same rationale.

***Claim Rejections - 35 USC § 103***

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. **Claims 6-8, 21-23, and 45-47** are rejected under 35 U.S.C. 103(a) as being unpatentable over '298 in further view of Carroll U.S. Patent No. 6,105,131 (hereinafter '131).

**As to dependent claim 21, "to provide a new file header; and storing the new file header at the file server"** is taught in '298 col. 6, lines 27-32 "Although PKC is referred in the embodiment of the present invention, any method of encryption is applicable. Next a medium signature 36 is created from the particular distribution medium on which COIN is encrypted with K1. It follows that the body 40 of the sealed COIN is generated. In step 68, the header is prepared next";  
the following is not taught in '298:

**"further comprising: encrypting the encryption key with a public key of a trusted third party; incorporating the encryption key encrypted with the public key of a trusted third party into the received file header"** however '131 teaches "A certificate (also called digital certificate) is an electronic credential issued by a trusted third party ... Encryption certificates provide certification of encryption keys used" in col. 4, lines 46-67.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system for controlling access to digital data of a file taught in '298 to include a means to issue keys by a trusted third party. One of ordinary skill in the art would have been motivated to perform such a modification to enhance security see '131 (col. 1, lines 29 et seq.) "Some web browsers provide a secured link by utilizing a security protocol, ... However, these safe guards fail to provide enough security".

**As to dependent claim 22, "further comprising: receiving a request"** is taught in '298 col. 11, line 1 "with an information consumer making an access request";

**“by the trusted third party to access the file; requesting access to the file by the trusted third party from the file server; receiving the encrypted file and the file header from the file server”** is taught in ‘131 col. 4, lines 9-13 “The computer network 14 connects user terminals 18 and RA terminal 16 to secure server 12 and third party terminals 66”.

**“extracting the encryption key encrypted with the public key of the trusted third party from the received file header; obtaining the private key of the trusted third party; decrypting the extracted encryption key encrypted with the public key of the trusted third party to recover the encryption key; and decrypting the encrypted file with the recovered encryption key”** is disclosed in ‘298 col. 7, lines 60-67 “the controller extracts in step 95 the encryption/decryption key ”.

As to dependent claim 23, **“further comprising: requesting the file header associated with the file from the file server; receiving the file header from the file server”** is taught in ‘298 col. 11, lines 1-11 “with an information consumer making an access request ... the information provider finds the corresponding key  $K_H$ , which it used in step 156 to encrypts the header fields 119”;

**“extracting the encryption key encrypted with the personal key and the control key; requesting recovery of the encrypted encryption key; receiving the recovered encrypted encryption key; generating the personal key; decrypting the recovered encrypted encryption key with the personal key to provide a recovered encryption key”** is shown in ‘298 col. 7, lines 60-67 “the controller extracts in step 95 the encryption/decryption key  $K_{TAL-LAL+1}$  from the header 35. The Controller 45”;

**“obtaining a new public key associated with the trusted third party”** is disclosed in ‘131 col. 4, lines 46-67 “A certificate (also called digital certificate) is an electronic credential issued by a trusted third party ... Encryption certificates provide certification of encryption keys”;

**“encrypting the recovered encryption key with the new public key to provide a new public key encrypted encryption key; incorporating the new public key encryption key in the file header to provide an updated file header; and providing the updated file header to the file server”** is taught in ‘298 col. 10, lines 47-65 “The information provider is ready to generate a Sealed-COIN in step 150 if it has CID and the values of the associated ... The header fields 119 in turn are encrypted in step 156 to form the header with a new key  $K_H$ ”.

**As to dependent claim 6-8**, these claims contain substantially similar subject matter as cited in the above claims 21-23 and are rejected along the same rationale.

**As to dependent claim 45-47**, these claims contain substantially similar subject matter as cited in the above claims 21-23 and are rejected along the same rationale.

7. **Claims 2, 30, and 55** are rejected under 35 U.S.C. 103(a) as being unpatentable over ‘298 in further view of Howard et al. U.S. Patent No. 6,678,731 (hereinafter ‘731).

**As to dependent claim 30, and rejecting the request if the authentication ticket is invalid”** is disclosed in ‘298 col. 11, lines 13-30 “If any of these checks fail, access to controlled information is denied”;

the following is not taught in ‘298:

**“wherein the request further includes an authentication ticket, the method further comprising the steps of: determining the validity of the authentication ticket however ‘731**

teaches “a request from a network server to authenticate a user who is seeking access ... The process determines whether the user was already authenticated by the authentication server” in col. 2, lines 44-55.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system for controlling access to digital data of a file taught in ‘298 to include a means to utilize an authentication server. One of ordinary skill in the art would have been motivated to perform such a modification to make information more easily available to valid users see ‘731 (col. 1, lines 50 et seq.) “If a user visits several different web sites, each web site may require entry of similar registration information about the user ... This repeated entry of identical data is tedious when visiting multiple web sites in a short period of time”.

**As to dependent claim 2, “and provide the ticket along with the file header to the personal key server and along with the encrypted file and the file header to the file server”** is shown in ‘298 col. 9, lines 7-10 “the encrypted COIN is packaged with some control data, which is called the “header” with the encrypted COIN is called the “body”. The header and body together are called the Sealed-COIN. A user presents the Sealed-COIN together with a ticket to the access device in order to access the COIN”;

**“wherein the personal key server is further configured to receive the ticket from the personal key client, determine the validity of the ticket and reject requests from the personal key client if the ticket is invalid; and wherein the file server is further configured to receive the ticket from the personal key client, determine the validity of the ticket and reject requests from the personal key client if the ticket is invalid”** is disclosed in ‘298 col. 11, lines 13-30 “If any of these checks fail, access to controlled information is denied”;

the following is not taught in '298:

**“further comprising: an authentication server configured to receive access requests from the personal key client, determine if the access request is authorized and provide a ticket to the personal key client if the access request is authorized; wherein the personal key client is further configured to request access from the authentication server, receive the ticket from the authentication server”** is taught in '731 col. 2, lines 44-55 “a request from a network server to authenticate a user who is seeking access ... The process determines whether the user was already authenticated by the authentication server”

As to **dependent claim 54**, this claim contains substantially similar subject matter as cited in the above claim 30 and is rejected along the same rationale.

*Conclusion*

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (703) 305-8917. The examiner can normally be reached on 6:30 am to 3:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A Morse can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 306-5484.

Ellen Tran  
Patent Examiner  
Technology Center 2134  
13 April 2004

  
NORMAN M. WRIGHT  
PRIMARY EXAMINER